Ph.D. Title Proposal

on

Leveraging Deepfake Technology for Financial Fraud: Detection and Prevention Strategies

Submitted in partial fulfillment of the requirement
for the award of the Degree of

Doctor of Philosophy

in

Information Technology

by

Mr. Akshay N. Shetye

under the guidance of

Dr. Nilakshi S. Jain

Department of Information Technology
Mahavir Education Trust's
Shah and Anchor Kutchhi Engineering College
Chembur, Mumbai-400088
University of Mumbai
August 2024

PROPOSAL FOR TOPIC APPROVAL TO BE SUBMITTED TO THE UNIVERSITY OF MUMBAI FOR THE DEGREE OF **Ph.D. (SCIENCE AND TECHNOLOGY)** IN THE SUBJECT OF **INFORMATION TECHNOLOGY**

Title of Topic	:	Leveraging Deepfake Technology for Financial Fraud: Detection and Prevention Strategies
Name of the Student	:	Mr. Akshay N. Shetye
Basic Qualification	:	M.E.(Computer Engineering) B.E.(Computer Engineering)
In the Case of Ph.D. student Year of Passing of PET/NET/SET/GATE (Teaching Experience)	:	GATE - 2021
Name of the Research Supervisor/ Guide	:	Dr. Nilakshi S. Jain
Date of Superannuation / Retirement	:	07/10/2046
Name of the Research Center	:	Shah and Anchor Kutchhi Engineering College
Signature of Student	:	
Signature of the Research Supervisor	:	

Seal of College

Head / Director / Principal
Research Centre

Sr. no.	Content	Page no.
1	Introduction	1
2	Rationale / Research Hypothesis	4
3	Aims & Objectives	4
4	Materials & Methods	5
5	Expected Results / Outcome	6
6	References	7

Statement by the Candidate

I wish to state that the work embodied in this synopsis titled “Leveraging Deepfake Technology for Financial Fraud: Detection and Prevention Strategies” forms my own contribution to the work carried out under the guidance of Dr.Nilakshi S. Jain at the Shah and Anchor Kutchhi Engineering College Chembur, Mumbai. I declare that this written submission represents my ideas in my own words and where others ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

(Candidate Signature)

Name: Mr. Akshay N. Shetye

Roll Number: 23DF18608IT005

Introduction

Recent years have witnessed a huge surge in digital payments.Worldwide, financial services have been made available to millions of people and various industries, businesses, and individual customers have benefited due to this rapid growth. In spite of these positive characteristics, digital payments have ushered in a new threat in the form of financial fraud or unauthorized payments . Financial fraud denotes the application of deceptive tactics or illegal and fraudulent means for obtaining financial benefits. Financial fraud, including money laundering, financial statement fraud, tax evasion, credit card fraud, and other forms of misconduct, is on the rise. These fraudulent activities are becoming increasingly sophisticated, leveraging advanced technologies to mislead and manipulate systems.. The rise of AI and Deepfake technologies enables fraudsters to create highly realistic fake identities, documents and communications, making traditional detection less effeffective. The recent case involving a Hong Kong-based firm illustrates a growing threat from Deepfake technology in the financial industry. Fraudsters used a Deepfake video to convincingly impersonate the firm's financial officer and other colleagues, leading an employee to mistakenly transfer US25million.

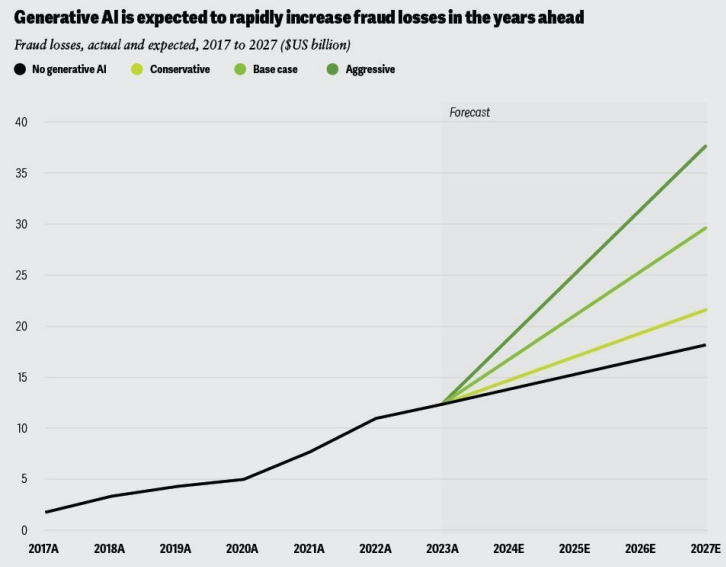

Figure 1: Financial Losses actual and expected from 2017 to 2027(in $US billion)

Source:www.deloitte.com

Many people have a tendency to take tips from investment advisor without making a actual research about investment in share market. Just imagine any fraudster make video of false investment advice through fake video as if featuring a well-known investment adviser himself .So, if such a videos spread over internet from attacker then lot of chances will be there that some investors will become victim of such a financial fraud. For such an attack fraudsters are looking to target prominent figures in the investment world, attempting to insist innocent investors to invest their money. Here are some cases of well-known personalities who were being dragged in such scam through their manipulated images, videos, speeches by an attacker.

- A doctor falls victim to a trading scam, losing Rs. 7 lakh after being deceived by an Instagram reel featuring a Deepfake of Mukesh Ambani.[Source:-The Economic Times]

- Sandeep Kumar, a resident of Greater Noida, lost Rs. 20.5 lakh in a work-from-home scam.[Source:- The Economic Times]
- Kerla man loses Rs. 40K to A.I. enabled deep fake fraud.[Source:-www.livemint.com]
- Narayan Murthy, founder of Infosys found in endorsement in automated trading application.[Source:- www.livemint.com]
- Deepfake video of Priyanka Chopra where priyanka's face and audio of her voice has been usedfor fake brand advertises.[Source:-www.livemint.com]
- Deepfake video of Sachin Tendulkar in promoting mobile application in Jan.2024.[Source:- www.livemint.com]
- Deepfake video of Norah Fatehi was appeared on a website of athletic shoes making company Lulumelon.[Source:-www.livemint.com]

Existing fraud detection systems often rely on rule based algorithms and anomaly detection which may not be effective against advanced Deepfake techniques. There is a need to develop innovative approaches that can identify and counteract Deepfake generated fraud. Financial fraud detection techniques aim at classifying financial statements into fraudulent or non-fraudulent. Generally, the approaches to detect fraud can be supervised or unsupervised. Recently, researchers have shown a heightened interest in utilizing machine learning techniques such as random forests, natural language processing, evolutionary algorithms, support vector machines (SVM), decision trees, neural networks, and logistic regression for the detection of corporate fraud. Lately, various new kinds of data apart from financial transactions have also been used in detecting financial fraud. Financial fraud detection can be carried out using various types of data and sources, such as historical records, account information, structured data from financial transactions, emails, text, audio recordings, video, and images. Researchers have specifically examined vocal features, like the voice characteristics of company executives, and linguistic features, such as their word choices, to detect fraud. This approach is based on the principle that valuable insights can be mined from both how people speak and the content of their speech. With the progress of generative AI, deep learning techniques can be used for curating content depending on the data on which they are trained. Hence, they can be used to detect frauds from text, audio, or video. These approaches have been widely exploited in video, audio and image recognition tasks and are found to cope up well with the huge volumes of data. These schemes learn by splitting the input data into multiple patterns using the hidden layers and are applied infraud detection .By considering all Deepfake cases; we can imagine how adverse it can in terms of financial frauds in future. There are following ways to generate and detect Deepfake Content .Various researchers proposed their work on Deepfake Technology

- Autoencoder- An Autoencoder is a deep learning algorithm that analyzes input data from various perspectives and conditions, and is capable of accurately replicating the original content.
- Generative Adversarial Network (GAN) -It is used to successful switch of identities of people by using random data. It consists of two main network namely Generator who generates candidates and discriminator who evaluate it.
- Style GAN-In 2014, it is been proposed and lot of improvement were made on Discriminator part of GAN to refine generators ability to generate content.

- Cycle GAN- It is used to transfer features of image to other image. Each Cycle GAN has 3 parts Encoder, Transformer and Decoder
- Big GAN-It is used to high resolution images and used in gaming
- SA-GAN(Self Attention Generative Adversarial Network)-Here an attention mechanism is used to focus on specific area of image.
- C-GAN(Conditional GAN)-In this GAN, we can incorporate specific input information, such as labels, class details, or other relevant features. This conditioning allows for more accurate and targeted data generation.
- Multi-modal GAN-Combine audio along with visuals to generate synchronized audio-visual content, for applications in video synthesis and lip-syncing.

There are various methods that address different challenges in Deepfake detection. Mainly there are two big approaches which played vital role in Deepfake detection, they are Audio Visual Deepfake detection where only audio and video type of data is considered and other is Multi-modal Deepfake Detection which involves multiple types of data beyond just audio and video, such as text, various physiological signals like eye movement, heart rate, lip movement, head movement, facial expression. There are various articles on Deepfake Technology in reputed journal which covers various aspects of it. A systematic Literature Review on Deepfake Detection Techniques and Deepfake video Detection: Challenges and Opportunities, elaborates all the techniques used to detect Deepfake content [8][6].In Speech Audio Deepfake Detection via Convolutional Neural Networks, idea of Deepfake audio detection by Convolutional Neural Network is explained well[10]. In 2021, through Fake Video Detection using Modified XceptionNet [7]a robust, adaptive and feature detection technique using ConvolutionalNeural Network is described. Articles like Joint Audio Video Deepfake Detection [23]and AVT2-DWF Improving Deepfake Detection With Audio-Visual Fusion and Dynamic Weighting Strategies[1] considered combination of audio and video to identify any inconsistency present in the content of video. Articles like Deepfake Detection Based on Discrepancies between Faces and their context[5], considers lip moment analysis to find any inconsistency ,Preventing Deepfake Attacks on Speaker Authentication by Dynamic Lip Movement Analysis,[6] Deepfake Detection with Enhanced Temporal and Spatial features[4][10] considers various biometric features of entities involved in the video to check originality ofthe content. In order to identify multiple identities varying face sizes,efforts were made to handle them in articles like MINTIME: Multiple Identity Size Invariant Video Deepfake Detection and Detection of Real Time Deepfake in Video Conferencing with Active Probing and Corneal Reflection[2][3].

Research Hypothesis

Based on objectives of Research ,we would like to propose following hypothesis.

- H1: Deepfake technology significantly increases the risk of financial fraud compared to traditional fraud methods.
- H2: Current fraud detection and prevention mechanisms are insufficient in addressing the unique challenges posed by Deepfake technology.
- H3: Implementing advanced detection frameworks and tools can substantially reduce the incidence of financial fraud enabled by Deepfake technology.

Aims & Objective

The Research aims to examine the impact of Deepfake technology on financial fraud. This involves exploring how Deepfake can facilitate financial fraud, understanding the underlying mechanisms, and devising effective strategies for detection and prevention.

- To Examine: Analyse current literature on deep fake technology and application of various Deep-fake types in financial fraud.
- To Evaluate: Assess the impact and consequences of financial fraud facilitated by deep fake technology on various stakeholders.
- To Develop and Validate: Propose frameworks, tool, and methodology for detecting financial fraud enabled by deep fake technology and validate its effeffectiveness of the proposed system.
- To Prevent: Propose methodologies for preventing Deepfake enabled Financial Fraud.

Materials & Methods

This work proposes a novel technique for Financial Fraud Detection using audio and video. Initially, the input audio/ video will be acquired from the dataset for the process of Deep fake financial fraud detection. If the input is audio, then the following steps will be performed: Primarily, the audio signal will be pre processed by using the Gaussian filter. Subsequently, feature extraction will be performed using Constant-Q Cepstral Coefficients (CQCC),Mel Frequency Cepstral Coefficients (MFCC), Cepstral Q Transform (CQT), and Mel spectrograms [27]. Finally, financial fraud detection using an audio signal will be performed by using WideResNet [29] with the Gannet Wolf Bird Optimization (GWBO), which will be developed by the combination of Gannet Optimization Algorithm (GOA) [27] and Wolf Bird Optimization (WBO) [28]. If the input is video, then the following steps will be performed: From the input video, the feature extraction will be carried out by using the Complete Local Binary Pattern (CLBP) [28], Local Binary Pattern (LBP) [21], and Pyramid Histogram of Oriented Gradients (PHOG) [28]. At last, the financial fraud detection video will be carried out by using WideResNet with GWBO. Moreover, the proposed WideResNet with GWBO for Financial Fraud Detection using audio and video will be implemented using the Python tool using the Deep Fake Video Classification dataset and AI Voice and Video Datasets - Speech Recognition Datasets. The effectiveness of the proposed WideResNet model integrated with GWBO will be evaluated using various metrics like,accuracy, precision, recall, Area Under the Curve (AUC), and the confusion matrix. Furthermore, the performance of this approach will be compared against current methods to demonstrate its comparative advantage.. Figure 2 shows the block diagram of the proposed WideResNet with GWBO for Financial Fraud Detection.

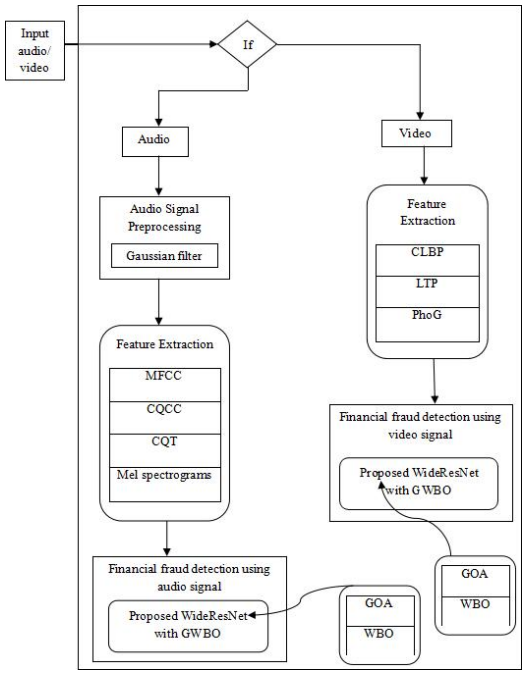

Figure 2: Block Diagram of Proposed System:-WideResNet with GWBO for financial fraud

Expected Results/Outcomes

- Enhanced Understanding: Improve comprehension and awareness of how Deepfake technology facilitates financial fraud.
- Detection Frameworks: Development of effective framework and tool for detecting Deepfake induced fraud.
- Preventive Strategy: Practical recommendations for preventing financial fraud involving Deepfake technology.

References

[1] Rui Wang , Dengpan Ye , Long Tang , Yunming Zhang , and Jiacheng Deng ”AVT2-DWF: Improving Deepfake Detection With Audio-Visual Fusion and Dynamic Weighting Strategies” in IEEE Signal Processing Letters,vol.31, 2024, pp. 1960-1964.

[2] Davide A. Coccomini , Giorgos K. Zilos, Giusepp.e Amato , Roberto Caldelli , Fabrizio Falchi , Symeon Papadopoulos , and Claudio Gennaro ”MINTIME: Multi-Identity Size-Invariant Video Deepfake Detection” in IEEE Transactions On Information Forensics And Security, vol. 19, 2024 ,pp. 6084-6095.

[3] Hui Guo, Xin Wang, and Siwei Lyu ”Detection Of Real-Time Deepfakes In Video Conferencing With Active Probing And Corneal Reflection” in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP-2023).

[4] Wenyuan Yang , Xiaoyu Zhou, Zhikai Chen, Bofei Guo, Zhongjie Ba ,Zhihua Xia , Xiaochun Cao , and Kui Ren ”AVoiD-DF: Audio-Visual Joint Learning for Detecting Deepfake” in IEEE Transactions On Information Forensics And Security, vol.18,2023 pp. 2015-2029.

[5] Yuval Nirkin , Lior Wolf, Yosi Keller , and Tal Hassner ”DeepFake Detection Based on Discrepancies Between Faces and Their Context” in IEEE Transactions On Pattern Analysis And Machine Intelligence, vol. 44, no. 10, 2022,pp. 6111-6121.

[6] Chen Z. Yang, Jun Ma, Shilin Wang, and Alan Wee-Chung Liew ”Preventing DeepFake Attacks on SpeakerAuthentication by Dynamic Lip Movement Analysis” in IEEE transactions on information forensics and security, vol. 16,2021,pp.1841-1854.

[7] Imam Kusniadi ,Arief Setyanto ”Fake Video Detection using Modified XceptionNet” in 4th International Conference on Information and Communications Technology (ICOIACT 2021).

[8] MC Weerawardana,TGI Fernando,”Deepfakes Detection Methods: A Literature Survey” in 10th International Conference on Information and Automation for Sustainability (ICIAfS-2021).

[9] TrongLe Do ,MaiKhiem Tran,Huy H. Nguyen,and MinhTriet Tran ”Potential Attacks of DeepFake on eKYC Systems and Remedy for eKYC with DeepFake Detection Using TwoStream Network of Facial App.earance and Motion Features” in SN Computer Science (2022) vol. 3, Issue 6,Sep 2022.

[10] Lucas P. Valente,Marcelo M. S. de Souza,Alan M. da Rocha ”Speech Audio Deepfake Detection via Convolutional Neural Networks” in IEEE International Conference on Evolving and Adaptive Intelligent Systems(EAIS-2024).

[11] Abdullahi U Ubale, Sunusi B. Abdullahi , Yu Liping , Bayan Alghofaily, Ahmed S. Almasoud , and Amjad Rehman ”Financial Fraud Detection Using Value-at-Risk With Machine Learning in Skewed Data” in IEEE Access vol .12,2024 ,pp. 64285-64299.

[12] Ranran Li , Zhaowei Liu , Yuanqing Ma, Dong Yang, and Shuaijie Sun ”Internet Financial Fraud Detection Based on Graph Learning” in IEEE Transactions on computational social systems, vol. 10, no.3, jun 2023 ,pp. 1394-1401.

[13] Sajjad Dadkhah , Xichen Zhang , Alexander Gerald Weismann, Amir Firouzi, and Ali A. Ghorbani ”The Largest Social Media Ground-Truth Dataset for Real/Fake Content: TruthSeeker ” in IEEE Transactions on computational social systems, vol. 11,no. 3,jun 2024,pp.3376-3390.

[14] J. Hendieh, M. Schneider, and T. Sakr, Fraud detection and prevention,Middle-East J. Sci.Res., vol. 31, no. 1, 2023., pp. 4452.

[15] Tomisin Awosika , Raj Shukla ,and Bernardi Pranggono ”Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection” in IEEE Access Vol 12 2024, pp. 64551-64560.

[16] Jesus, S., Pombal, J., Alves, D., Cruz, A., Saleiro, P., Ribeiro, R., Gama, J., and Bizarro, P. (2022). Turning the tables: Biased, imbalanced, dynamic tabular datasets for ML evaluation. In Proc. Adv. Neural Inf. Process. Syst., vol. 35, pp. 33563-33575.

[17] M. J. Rahman and X. Jie, Fraud detection using fraud triangle theory:Evidence from China, J. Financial Crime, vol. 31, no. 1, ,Jan. 2024,pp. 101118.

[18] S. Sharma, R. K. Gupta, and A. Verma, ”Real-Time Fraud Detection in Financial Transactions Using Big Data Analysis,” 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL,USA, 2021, pp. 123-132.

[19] Y. B. Lin and Y. C. F. Wang, Audiovisual transformer with instance attention for audio-visual event localization, in Proc. Asian Conf.Comput. Vis., 2020, pp. 117.

[20] T. Mittal, U. Bhattacharya, R. Chandra, A. Bera, and D. Manocha, Emotions dont lie: An audio-visual deepfake detection method usingaffective cues, in Proc. ACM Int. Conf. Multimedia, Oct 2020,pp. 28232832.

[21] Wang, H., Wang, W., Liu, Y., and Alidaee, B. . Integrating machine learning algorithms with quantum annealing solvers for online fraud detection. IEEE Access, 2022 vol.10, pp.75908-75917.

[22] D. Sisodia and D. S. Sisodia, Data sampling strategies for click fraud- detection using imbalanced user click data of online advertising: An empir$_x$0002$_i$*calreview, IETETech.Rev., vol.*39*, no.*4*, , Jul.*2022*, pp.*789798*.*

[23] T.-C. Wang, ”Avoid-DF: Audio-Visual Joint Learning for Detecting Deepfake,” 2021 IEEE Confer- ence on Computer Vision and Pattern Recognition (CVPR), Nashville, TN, USA, 2021, pp.1234-1243.

[24] G. Moschini, R. Houssou, J. Bovay, and S. Robert-Nicoud, Anomaly and fraud detection in credit card transactions using the ARIMA model, in Proc. 7th Int. Conf. Time Forecasting, Jul. 2021, pp. 56-64.

[25] Alexandros Haliassos, Konstantinos Vougioukas ,Stavros Petridis1and Maja Pantic Lips Dont Lie: A Generalisable and Robust App.roach to Face Forgery in IEEE/CVF Conference on Computer Vision and Pattern Recognition pp. 5037-5047.

[26] T. Zhao, X. Xu, M. Xu, H. Ding, Y. Xiong, and W. Xia, Learning Self-Consistency for Deepfake Detection, in Proc. IEEE Conf. Comput.Vis. Pattern Recognit., Oct. 2021, pp. 15023-15033.

[27] Wani, T.M., Qadri, S.A.A., Comminiello, D. and Amerini, I., Detecting Audio Deepfakes: Integrating CNN and BiLSTM with Multi-Feature Concatenation, In Proceedings of the 2024 ACM Workshop on Information Hiding and Multimedia Security, June 2024 pp. 271-276.June 2024 pp. 271-276.

[28] Azizi, M., Shishehgarkhaneh, M.B., Basiri, M., Moehler, R.C., Fang, Y. and Chan, M.,Wolf-Bird Optimizer (WBO): A novel metaheuristic algorithm for Building Information,Modeling-based resource tradeoff Journal of Engineering Research, 2023.

[29] Hu, S., Zhang, B., Lu, J., Jiang, Y., Wang, W., Kong, L., Zhao, W. and Jiang, T.,WideResNet with Joint Representation Learning and Data Augmentation for Cover Song Identification, In Interspeech,September. 2022 pp. 4187-4191.

[30] Pan, J.S., Zhang, L.G., Wang, R.B., Snel, V. and Chu, S.C., Gannet optimization algorithm: A new metaheuristic algorithm for solving engineering optimization problems, Mathematics and Computers in Simulation,2022 vol. 202, pp.343-373.

[31] Ahmadi, S., Open AI and its Impact on Fraud Detection in Financial Industry, Journal of KnowledgeLearning and Science Technology ISSN, 2023,pp.2959-2983 .